

**WHITE & CASE LLP**

J. Christopher Shore  
Philip Abelson  
David Turetsky  
Michele J. Meises  
1221 Avenue of the Americas  
New York, NY 10020  
Telephone: (212) 819-8200  
Facsimile: (212) 354-8113

– and –

Gregory F. Pesce (admitted *pro hac vice*)  
111 South Wacker Drive, Suite 5100  
Chicago, IL 60606-4302  
Telephone: (312) 881-5400  
Facsimile: (305) 881-5450

*Proposed Counsel to Official Committee of Unsecured Creditors*

**UNITED STATES BANKRUPTCY COURT  
SOUTHERN DISTRICT OF NEW YORK**

In re:

Genesis Global Holdco, LLC, *et al.*,<sup>1</sup>

Debtors.

Chapter 11

Case No.: 23-10063 (SHL)

Jointly Administered

**Re: Docket No. 137, 156, 157**

**SUPPLEMENTAL DECLARATION OF MARK RENZI IN SUPPORT  
OF THE OFFICIAL COMMITTEE OF UNSECURED CREDITORS' MOTION  
FOR ENTRY OF AN ORDER REQUIRING THE REDACTION  
OF CERTAIN PERSONALLY IDENTIFIABLE INFORMATION**

I, Mark Renzi, declare pursuant to 28 U.S.C. § 1746 as follows:

<sup>1</sup> The Debtors in these chapter 11 cases, along with the last four digits of each Debtor's tax identification number (as applicable), are: Genesis Global Holdco, LLC (8219); Genesis Global Capital, LLC (8564); Genesis Asia Pacific Pte. Ltd. (2164R). For the purpose of these chapter 11 cases, the service address for the Debtors is 250 Park Avenue South, 5th Floor, New York, NY 10003.

1. I am a Managing Director at, and the Head of Corporate Finance Financial Institutions Group for, Berkeley Research Group, LLC (“**BRG**”). BRG is the proposed financial advisor to the Official Committee of Unsecured Creditors (the “**Committee**”) appointed in the cases of the above-captioned debtors and debtors in possession (collectively, the “**Debtors**”).

2. I respectfully submit this supplemental declaration (the “**Declaration**”) in further support of *The Official Committee of Unsecured Creditors’ Motion for an Order Requiring the Redaction of Certain Personally Identifiable Information* [Docket No. 137] (the “**Motion**”). This Declaration supplements my initial declaration in support of the Motion [Docket No. 156] (the “**Initial Declaration**”), incorporated fully herein by reference,<sup>2</sup> in order to address certain statements made by the Office of the United States Trustee for Region 2 (the “**U.S. Trustee**”) in the *Omnibus Objection of the United States Trustee to: (A) the Debtors’ Motion Seeking the Redaction or Sealing of Certain Information [and] (B) the Unsecured Creditors’ Committee’s Request to Seal Certain Information* [Docket No. 157] (the “**U.S. Trustee Objection**”) and in support of *The Official Committee of Unsecured Creditors’ Reply to Objection of United States Trustee and in Support of Committee’s Motion for an Order Requiring the Redaction of Certain Personally Identifiable Information* (the “**Reply**”), filed contemporaneously herewith. I am authorized to submit this Declaration on behalf of the Committee.

3. The statements made in this Declaration are based upon my personal knowledge, my review of relevant documents, information provided to me by other professionals in these cases and/or employees working under my supervision, or my opinion based upon my experience, knowledge, and information concerning the Debtors’ operations. I declare the following

---

<sup>2</sup> Capitalized terms used but not otherwise herein defined shall have the meanings ascribed to such terms in the Motion or the Initial Declaration, as applicable.

statements are true to the best of my knowledge, information, and belief formed after a reasonable inquiry under the circumstances.

4. I am over the age of 18 and authorized to submit this Declaration on behalf of the Committee. If called as a witness, I would testify truthfully to the matters stated in this Declaration.

**Creditors Have Raised Particularized Concerns in Response to the U.S. Trustee Objection**

5. My Initial Declaration stated that the value of the Confidential Information (which consists of the names, physical addresses, and e-mail addresses of the Debtors' lenders) to the Debtors' estates depends upon the Confidential Information being kept private and confidential. As described in my Initial Declaration, unfettered access to the Confidential Information will provide potential transaction counterparties and competitors with access to the Confidential Information, which, in turn, would allow those potential transaction counterparties and competitors to contact and poach the Debtors' lenders without providing any compensation to the estates. Initial Declaration ¶¶ 12–17.

6. In my Initial Declaration, I also expressed my belief that disclosure of the Confidential Information would place the Debtors' creditors at risk. *Id.* ¶¶ 18–22. In light of subsequent developments, my belief that the Debtors' creditors could face risk of harm (including potential financial, psychological, or physical harm) has become stronger. More specifically, since the filing of the Motion and my Initial Declaration, numerous creditors have contacted the Committee or its professionals regarding the relief requested in the Motion and the arguments made in the U.S. Trustee Objection. Based on my review of those communications and discussions with members of the Committee, I believe that the disclosure of the Confidential Information will credibly place certain creditors at risk of blackmail, kidnapping, and other forms

of financial, psychological, or physical harm. Those risks are particularly salient here because it is my understanding that substantially all of Genesis's investors qualify as accredited investors who are high net worth individuals. This is relevant because there is a greater risk that criminals or other bad actors will attempt to inflict financial, psychological, or physical harm of high network individuals than other individuals by using coercion to access their cryptocurrency or other digital assets. Based on my understanding of the Debtors' business enterprise, I believe that the mere risk of such potential financial, psychological, or physical harm would impair the value of the Confidential Information (which the Debtors seek to monetize through their marketing process). I also believe that the mere risk of such potential financial, psychological, or physical harm will impair the goodwill between the Debtors and their lenders, which would further undermine the value of the Confidential Information and thus impair creditor recoveries in these cases.

**I. Federal and State Agency Warnings to Cryptocurrency Holders.**

7. In addition to my review of communications between various lenders and the Committee regarding this topic, my belief regarding the relief requested in the Motion is enhanced by my experience in other cryptocurrency bankruptcy engagements, my review of publicly available information on the topic, and other knowledge of the industry.

8. More specifically, numerous federal law enforcement and administrative agencies have issued public statements in the form of official alerts, bulletins, and press releases expressly warning of tactics, schemes, and incidents of theft and/or violence against cryptocurrency owners as well as executives of cryptocurrency companies. For example, the Federal Bureau of Investigation (the "**FBI**") has issued warnings regarding the increasing use of Subscriber Identity Mobile (SIM) swap scams, whereby criminals that are able to obtain cellphone SIM cards from

victims and steal their personal information. SIM swap scams involve criminals that are able to obtain an individual's SIM card through phishing tactics by pretending to be the victim's mobile carrier. In SIM swap scams, once the SIM is swapped, the victim's calls, texts, and other data are diverted to the criminal's device, allowing the criminal to send "Forgot Password" or "Account Recovery" requests to the victim's e-mail and other online accounts associated with the victim's phone profile.

9. True and accurate copies of reports of various warnings issued by the FBI and other agencies urging the public not to advertise financial ownership in cryptocurrency or other financial assets are attached to this Declaration. Those reports are summarized as follows:

- On February 8, 2022, the FBI issued a public service announcement to inform the public of the "increasing use of Subscriber Identity Module (SIM) swapping by criminals to steal money from fiat and virtual currency accounts." The FBI specifically recommended that individuals take certain precautions to protect against theft, including to "not advertise information about financial assets, including ownership or investment of cryptocurrency" and "avoid posting personal information online, such as mobile phone number, address, or other personal identifying information." See Exhibit [A].
- In September 2022, the U.S. Department of the Treasury published a report entitled *Crypto-Assets: Implications for Consumers, Investors, and Businesses* highlighting certain risks posed by cryptocurrency, including theft, which accounted for \$3.2 billion of "crypto-asset-based crime" in 2021 through security breaches such as phishing, key logging, and social engineering. See Exhibit [B].
- In May 2022, the Federal Trade Commission (the "FTC") published a Consumer Advice article entitled *What To Know About Cryptocurrency and Scams*, which warned of, among other things, blackmail scams involving "emails or U.S. mail sent to [an individual's] home" threatening to make information public unless they are paid in cryptocurrency. See Exhibit [C].
- On November 10, 2022, the Consumer Financial Protection Bureau published a bulletin highlighting complaints it had received related to crypto-assets and warning consumers about SIM-swapping, phishing, and other types of hacking. See Exhibit [D].

- On June 24, 2022, the United States Attorney’s Office for the Southern District of New York issued a press release detailing the unsealed indictment of two defendants charged under a federal conspiracy statute in connection with “a violent plan to break into a family’s home in the middle of the night and force its residents to provide the code to what the defendants believed was tens of millions of dollars in Bitcoin currency.” See Exhibit [E].
- On January 20, 2022, U.S. Customs and Border Protection issued a national media release warning of various telephone phishing scams involving criminals impersonating U.S. Border Patrol agents who, among other tactics, request that an individual provide information in exchange for Bitcoin. See Exhibit [F].
- On October 19, 2022, the United States Department of Justice (the “DOJ”) issued a press release detailing the arrest and conviction of two defendants who targeted, among others, “executives of cryptocurrency companies and others who likely had significant amounts of cryptocurrency” in a scheme in which approximately \$330,000 was stolen through “SIM swapping,” computer hacking, and other methods. See Exhibit [G].
- On April 13, 2020, the FBI issued a press release warning of an increase in certain cryptocurrency fraud schemes related to the COVID-19 pandemic, including blackmail attempts. See Exhibit [H].
- On June 3, 2022, the FTC published a blog post highlighting that, “since 2021, more than 46,000 people have reported losing over \$1.0 billion in crypto to scams.” See Exhibit [I].

## **II. Documented Instances of Threatened and Actual of Physical Violence Highlight the High-Stakes Nature of Disclosing the Confidential Information.**

10. In addition, I believe that the potential disclosure of the Confidential Information may lead to kidnapping and other forms of physical violence against creditors. True and accurate copies of various articles describing examples of violent incidents as reported by various news outlets across the world are attached to this Declaration and are summarized as follows:

- In a 2018 article entitled *Bitcoin Thieves Threaten Real Violence for Virtual Currencies*, the New York Times described the “startling” number of bitcoin thieves threatening real violence to force cryptocurrency holders to transfer assets through irreversible transactions. For example, in New York City, a man was held captive by a friend until he transferred over \$1.8 million worth of Ether, and in Phuket, Thailand, a young man was attacked in his apartment until he transferred \$100,000 worth of bitcoin to a wallet that the attackers controlled. See Exhibit [J].

- The crypto-focused news outlet CoinTelegraph highlighted in 2022 that “\$5 wrench attacks,” or attacks on known holders of significant sums of cryptocurrency, appear to be on the rise. See Exhibit [K].
- In Bali, Indonesia, a group of four men attacked a known cryptocurrency investor at his home, beating him and forcing him to transfer \$284,000 worth of bitcoin to his assailants. See Exhibit [L].
- In Manerba, Italy, a known owner of cryptocurrency became the target of robbers, who held the victim at knifepoint while forcing him to transfer cryptocurrency to the robbers’ accounts. See Exhibit [M].
- In Madrid, Spain, the president and founder of a social media company was handcuffed and gagged in his apartment by assailants who extorted him for several hours in an effort to obtain the password to his accounts holding several millions in euros in bitcoin. See Exhibit [N].
- In Kyoto, Japan, several men confined and beat the son of the former CEO of Mitsubishi Electric who was known to be holding cryptocurrency in an effort to force him to transfer the crypto tokens to the assailants. See Exhibit [O].
- In Hong Kong, a known cryptocurrency trader was lured and held against his will and beaten by suspected gang members attempting to force him to pay them HK\$30 million cryptocurrency as ransom. See Exhibit [P].
- In Kiev, Ukraine, a cryptocurrency investor was beaten and tortured for three hours by three men who were aware of this cryptocurrency holdings in an effort to extort him. See Exhibit [Q].

11. I believe that disclosure of the Confidential Information poses a credible risk of financial, psychological, or physical harm to individual lenders and the individuals associated with institutional lenders. This conclusion is informed by the evidence attached hereto. The risk of financial, psychological, or physical harm could be minimized, however, by requiring the redaction of the Confidential Information of (a) individual lenders, as contemplated by the Creditor Matrix, the Redaction Motion, and the Motion; and (b) institutional lenders, as specifically requested by the Motion.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Dated: March 29, 2023

/s/ Mark Renzi

Mark Renzi  
Berkeley Research Group, LLC

*Proposed Financial Advisor to the  
Committee*